CLAIMS

1. A method for analyzing a security event in a distributed fashion, comprising:

(a) detecting an occurrence of a security event within a customer network;

(b) querying a first component of the customer network for data in response to the detected occurrence of the security event;

(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query;

(d) determining, based on the received first data, whether to query for additional data;

(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step; and

(f) analyzing the security event using at least one of the first data and the additional data.

2. The method of claim 1 wherein step (a) further comprises determining at least one of intrusion of the customer network, a port scan, service probes, a signature from an attack, a buffer overflow attempt, a format string attack, a denial of service attempt, a web-based attack, and an attempted rights escalation.

3. The method of claim 1 wherein step (a) further comprises monitoring the customer network for the security event.

4. The method of claim 1 wherein step (a) further comprises determining at least one of nature of the security event, likelihood that the security event is harmful, and impact of the security event.

5. The method of claim 1 wherein step (a) further comprises detecting, by the data monitor, the occurrence of the security event.

6. The method of claim 1 wherein the security event further comprises a potential security event.

7. The method of claim 1 wherein at least one of the first component and the another component of the customer network further comprises at least one of the data monitor and a client computer.

8. The method of claim 1 wherein step (b) further comprises querying, by the data monitor, the component.

9. The method of claim 1 wherein step (c) further comprises at least one of

(i) transmitting the received first data to a security analysis module for analysis, and

(ii) analyzing the first data.

10. The method of claim 1 wherein step (d) further comprises analyzing the first data to determine whether to query for additional data.

11. The method of claim 1 wherein step (d) further comprises determining, by the data monitor, whether to query for additional data.

12. The method of claim 1 wherein step (f) further comprises populating a trouble ticket during the analysis.

13. The method of claim 1 wherein step (f) further comprises analyzing, by the data monitor, the security event.

14. The method of claim 1 further comprising reporting a result of the analysis.

15. A method for analyzing a security event in a distributed fashion, comprising:

(a) detecting an occurrence of a security event within a customer network;

(b) querying a first component of the customer network for data in response to the detected occurrence of the security event;

(c) receiving, by a data monitor located within the customer network, first data from the component in response to the query;

(d) determining, based on the received first data, whether to query for additional data;

(e) querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step; and

(f) analyzing, by the data monitor, the security event using at least one of the first data and the additional data.

16. An apparatus for analyzing a security event within a customer network comprising:

(a) a data monitor, positioned within the customer network, to collect data from at least one component of the customer network in response to a query; and

(b) a security analysis module, in communication with the data monitor, to detect an occurrence of the security event, wherein the security analysis module comprises:

(b-a) a receiver for receiving data from the data monitor,

(b-b) an analyzer, in communication with the receiver, for analyzing the security event, and

(b-c) a querying module, in communication with the analyzer, for querying the data monitor for data repeatedly until the analyzer can analyze the security event using the data.

17. The apparatus of claim 16 wherein the querying module further comprises at least one of a query processor, an analyst, a message router, and a resolver.

18. The apparatus of claim 16 wherein the component further comprises a client located within the customer network.

19. The apparatus of claim 16 further comprising an analyst to at least one of

(i) modify settings of the data monitor in response to at least one of the security event, a query, and the data,

(ii) monitor communications between the data monitor and the security analysis module,

(iii) initiate the query of the data monitor, and

(iv) modify the query of the querying module.

20. The apparatus of claim 16 wherein the security analysis module further comprises at least one of

(b-d) an event repository to store information about the security event,

(b-e) a message router, in communication with the querying module, to direct and receive at least one of queries and the data, and

(b-f) a resolver, in communication with the querying module, to provide a location of at least one of the data monitor and the component to the querying module.

21. The apparatus of claim 20 wherein the resolver further comprises a characteristic table having an attribute of a component in the customer network.

22. The apparatus of claim 21 wherein the attribute of the component further comprises at least one of type of service provided to the component, company that the component resides in, network address of the component, geographic data of the component, security domain of the component, and information of a service level agreement associated with the component.

23. The apparatus of claim 16 further comprising an arbitrator that prioritizes at least one of the security event in a plurality of security events and the data received from the data monitor.

24. The apparatus of claim 23 wherein the arbitrator further comprises at least one of

(i) a threat analysis engine analyzing the security event based on a parameter of the security event to determine importance of the security event,

(ii) a business asset analysis engine determining an impact of the security event if left unresolved; and

(iii) a service level management engine determining steps needed to resolve the security event.

25. The apparatus of claim 24 wherein the parameter of the security event further comprises at least one of amount of time elapsed since the occurrence of the security event, duration of time of the security event, number of previous occurrences of the security event, communication protocol, and type of security event.

26. The apparatus of claim 24 wherein the impact determined by the business asset analysis engine further comprises at least one of a down time that a component of the customer network may experience in response to the security event, costs associated with the down time, and estimated man-hours to resolve the security event.

27. The apparatus of claim 24 wherein the steps needed to resolve the security event further comprise determining a resolution time for the security event.

28. The apparatus of claim 16 wherein at least one of the security analysis module, the receiver, the analyzer, and the querying module are located on the customer network.

29. The apparatus of claim 16 wherein the data monitor further comprises at least one of

(i) a security defense appliance monitoring the customer network,

(ii) a security management appliance, in communication with the security defense appliance, receiving a query from the querying module and directing the query to the security defense appliance, and

(iii) a security analysis appliance analyzing the data.

30. An apparatus for analyzing a security event within a customer network comprising:

(a) a data monitor, positioned within the customer network, to collect data from the customer network; and

(b) a security analysis module, in communication with the data monitor, to determine an occurrence of the security event;

(c) a receiver for receiving data from the data monitor,

(d) an analyzer, positioned within the customer network, for analyzing the security event, and

(e) a querying module, in communication with the analyzer, for querying the data monitor for data repeatedly until the analyzer can analyze the security event using the data.

31. The apparatus of claim 30 wherein the data monitor further comprises at least one of

(i) a security defense appliance monitoring the customer network,

(ii) a security management appliance, in communication with the security defense appliance, receiving a query from the querying module and directing the query to the security defense appliance, and

(iii) a security analysis appliance analyzing the data.

32. The apparatus of claim 32 wherein the analyzer further comprises the security analysis appliance.

33. The apparatus of claim 31 wherein at least one of the security analysis module, receiver, and querying module are located within the customer network.